平成２３年度
情報セキュリティ報告書

平成２４年５月

国土交通省

目次

１．最高情報セキュリティ責任者によるメッセージ及び当該年度の総括

１．１．はじめに　～最高情報セキュリティ責任者からのメッセージ～

経済活動や社会・国民生活の多くの面において情報通信技術の利用が一層進む中、情報セキュリティ上のリスクが多様化・高度化しており、情報通信技術を安全・安心に活用するための取組が必要不可欠となっています。また、昨今の情報窃取を目的として、特定の組織や個人に送られる標的型メールによるサイバー攻撃等の新たな情報セキュリティ上の脅威に対しても適切に対応していく必要があります。

国土交通省は、国土の開発利用保全、社会資本の整備、交通政策の推進、気象、海上の安全・治安確保等、広範な分野を担当するとともに、外局や地方支分部局を含め多様な機能を持つ組織を擁する機関です。このため、組織全体として適切な情報セキュリティ対策を実施していくことは極めて重要であります。

従来より、国土交通省情報セキュリティポリシーの制定及び運用を通じ、省内の体制構築と責任の明確化、状況の変化に応じた継続的な取組等、情報セキュリティ対策の徹底に努めてきました。

本報告書は、平成２３年度に国土交通省が実施した情報セキュリティ対策に対する取組状況、その結果等についてとりまとめたものです。

情報セキュリティ対策を実施する上では、各部局において取扱う情報の内容や業務の実態を踏まえ、柔軟かつ適切な対策・措置を図ることが重要です。今後も、情報の取扱い、情報システムの適切な運用について、全職員に周知徹底するとともに、新しい脅威に対する適切な対策を講じ、引き続き情報セキュリティ対策の維持・強化に努めて参ります。

最高情報セキュリティ責任者
（国土交通省総合政策局長）
中島　正弘

１．２．平成２３年度の総括

（１）平成２３年度の評価

（ア）セキュリティ対策実施状況に関する自己点検結果

国土交通省では、年度自己点検計画に基づき、全職員を対象として情報セキュリティ対策実施状況に関する自己点検を実施したところ、概ね適切に対策を実施していることが明らかになりました。

今後は、引き続き今年度の水準を維持するとともに、比較的低い結果となっている分野について重点的に改善を検討し、さらなる向上を目指して参ります。

（イ）情報システムごとの状況

国土交通省における各情報システムのセキュリティ対策について、あらかじめ配布した検査項目に則って調査を実施した結果、情報システムを構成する公開Ｗｅｂサーバ、電子メールサーバ及びＤＮＳサーバにおいて、適切な対策が実施されていることが明らかになりました。

今後もこの状態を維持できる様、引き続き情報セキュリティ対策の実施に努めて参ります。

（ウ）教育・啓発

国土交通省では、情報セキュリティに関して職員が守るべきルールを「国土交通省情報セキュリティポリシー」（以下「情報セキュリティポリシー」という）や「国土交通省行政情報システム管理運営規則」として定め、イントラネット経由で省内職員に配信しています。また、特に重要なポイントについて「情報セキュリティ確保のためのお役立ち５つのポイント」として整理し、職員に対して頻繁にポップアップメッセージを表示する等により周知徹底を図り、情報セキュリティに関する研修を実施することにより、情報セキュリティ対策に対する各職員の理解の向上に努めています。

また、不審メール対策として、省庁職員になりすまして送信される不審メールについてもポップアップメッセージ等による注意喚起を行っています。

（エ）調達・外部委託

国土交通省では「外部委託における情報セキュリティ対策実施規程」を定め、外部委託により行う情報処理業務の遂行における情報セキュリティ対策等を委託契約に含めることで、情報セキュリティ確保のための事項を委託先に確実に行わせ、必要な情報セキュリティ水準を確保しています。なお、当規程についてはイントラネットに掲載すること等により、各職員へ周知しています。

（オ）情報セキュリティに関する障害・事故等の報告

国土交通省では、情報セキュリティに関する障害・事故等が平成２３年度６件発生しましたが、速やかに適切な対策を実施しました。

（２）平成２４年度の課題

国土交通省では、今年度に引き続き自己点検や監査等を着実に実施するとともに、来年度重点的に取組む課題を以下のとおりとし、今後さらなる情報セキュリティの向上を目指します。

○情報の不適切な利用や持ち出し等による情報漏えいを防止するため、ライフサイクルごとに情報の格付けに応じた適切な取扱いの徹底を行います。

○情報セキュリティを取り巻く環境の変化に応じた点検項目の設定や点検内容を正確に理解してもらうために更なる見直しを行います。また、外局や地方支分部局を含め省内全ての部局において実施している部局内監査について、より効率的・効果的なものとなるよう見直しを行います。

○情報セキュリティ対策の実施効果を一層高めるためには、全職員に対して対策や措置内容を分かりやすい形で周知・徹底することが重要です。職員に対し従前より実施している「情報セキュリティ確保のためのお役立ち５つのポイント」や不審メール対策に関する周知等について、内容の改善も図りながら今後も継続的に実施します。

２．報告書の基本情報

２．１．国土交通省の概要

国土交通省は、国土の総合的かつ体系的な利用、開発及び保全、そのための社会資本の整合的な整備、交通政策の推進、観光立国の実現に向けた施策の推進、気象業務の健全な発達並びに海上の安全及び治安の確保を図ることを任務としています。

国土交通省では、これらの業務の継続的かつ安定的な実施を確保するために必要な情報システムを構築し運用しています。

２．２．対象とする期間

本報告書は、平成２３年４月１日から平成２４年３月３１日の期間の国土交通省における情報セキュリティ対策の取組を対象としています。

２．３．対象とする組織

本報告書は、国土交通省の本省、特別の機関（国土地理院、小笠原総合事務所、海難審判所）、施設等機関（国土交通政策研究所、国土技術政策総合研究所、国土交通大学校、航空保安大学校）、地方支分部局（地方整備局、北海道開発局、地方運輸局、地方航空局、航空交通管制部）及び外局（観光庁、気象庁、運輸安全委員会、海上保安庁）を対象としています。

２．４．対象とする情報

本報告書で対象とする情報は、情報セキュリティポリシーで対象としている情報とします。具体的には、国土交通省における情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び電磁的に記録された書面に係る情報であって、国土交通省行政文書管理規則（平成２３年国土交通省訓令第２５号）第２条第１号に規定する行政文書に係るもの（情報システムに関する設計書を含む）とします。

２．５．本報告書の責任部署

本報告書の責任部署は、国土交通省総合政策局情報政策課です。

３．情報セキュリティ対策の枠組み

３．１．情報セキュリティ対策に関する文書体系

国土交通省では、「政府機関の情報セキュリティ対策のための統一基準群」（以下「政府統一基準群」という。）に基づき情報セキュリティポリシーを策定し、①地方支分部局、外局等を含む省内の体制を整備し、責任関係を整理するとともに、②情報の格付け基準や格付けに応じた情報の取扱方法（アクセス制御や保存・移送の方法など）等を詳細に規定しました。この情報セキュリティポリシーに基づき、国土交通省における情報及び情報システムをあらゆる脅威から守るために必要な情報セキュリティ確保に最大限取組んでいます。具体的に実施すべき対策については、基本遵守事項及び強化遵守事項として定めています。

また、情報セキュリティポリシーに定められた遵守事項を運用していくための具体的な手順となる文書として、以下の規程等を整備しています。さらに、各部局においては、必要に応じて情報セキュリティポリシーの具体的な実施手順を策定し、運用しています。

［国土交通省情報セキュリティ関係規程］

○　情報の格付け及び取扱制限に関する規程
○　例外措置手順
○　人事異動の際に行うべき情報セキュリティ対策実施規程
○　機器等の購入における情報セキュリティ対策実施規程
○　外部委託における情報セキュリティ対策実施規程
○　国土交通省支給以外の情報システムによる情報処理に関する安全管理措置規程
○　国土交通省外の情報セキュリティ水準の低下を招く行為の防止に関する規程
○　障害・事故等報告及び対処手順
○　国土交通省外での情報処理の制限に関する規程
○　ソフトウェア開発における情報セキュリティ対策実施規程
○　暗号と電子署名に係る規程
○　ドメイン名の使用に関する規程
○　不正プログラム対策に係る規程
○　情報セキュリティ監査実施手順

３．２．情報セキュリティ対策の推進体制

（１）国土交通省における情報セキュリティ対策に係る組織体制

情報セキュリティ対策は、それに係るすべての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で負うべき責務を全うすることで実現されます。そのため、それらの権限と責務を明確にし、必要となる組織や体制を整備する必要があります。

以上のことを勘案し、国土交通省では、情報システム及び情報セキュリティ対策を推進するため、政府統一基準群及び情報セキュリティポリシーに基づき、以下の図１に示す体制を整備しています。

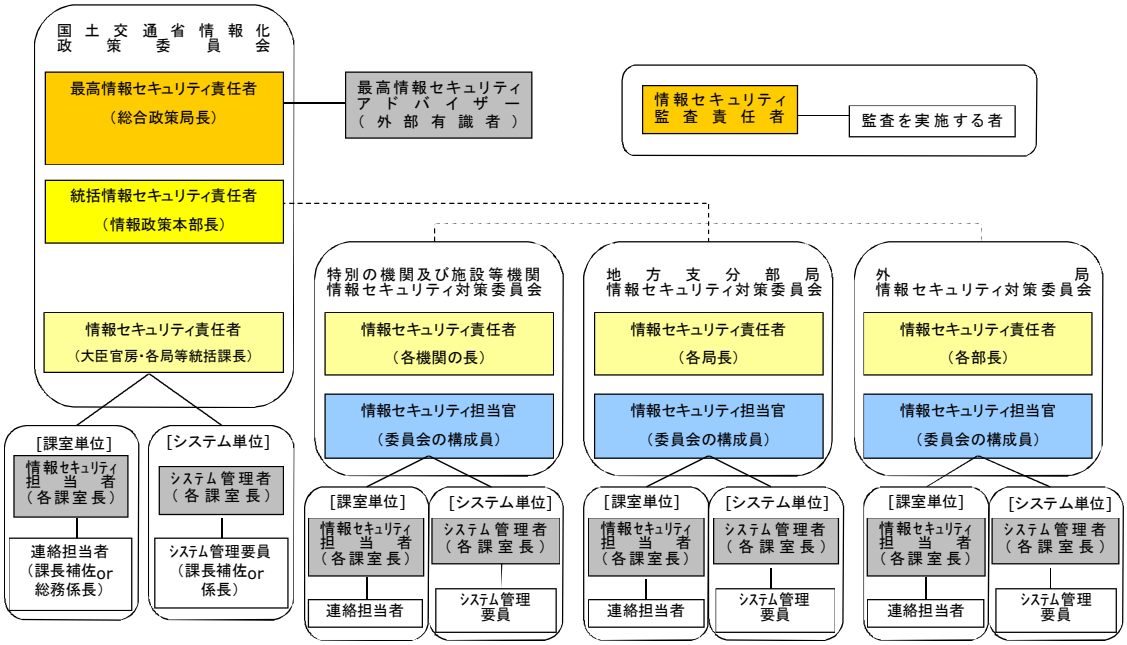

図１　国土交通省における情報セキュリティ対策の推進体制

○　国土交通省情報化政策委員会

　情報セキュリティポリシーの承認等重要事項の決定を行い、重要事項に関する関係部署との連絡及び調整を行うため、国土交通省情報化政策委員会を設置しています。最高情報セキュリティ責任者である総合政策局長が委員会の長を務めています。

○　特別の機関及び施設等機関情報セキュリティ対策委員会

　国土交通政策研究所、国土技術政策総合研究所、国土交通大学校、航空保安大学校、国土地理院、小笠原総合事務所及び海難審判所（以下「特別の機関及び施設等機関」という。）は、特別の機関及び施設等機関の長を委員長とする特別の機関及び施設等機関情報セキュリティ対策委員会を設置し、情報セキュリティポリシーの推進を図っています。

○　地方支分部局情報セキュリティ対策委員会

　各地方整備局、北海道開発局、各地方運輸局、各地方航空局及び各航空交通管制部（以下「地方支分部局」という。）は、それぞれ地方支分部局の長を委員長とする地方支分部局情報セキュリティ対策委員会を設置し、情報セキュリティポリシーの推進を図っています。

○　外局情報セキュリティ対策委員会

　観光庁、気象庁、運輸安全委員会及び海上保安庁（以下「外局」という。）は、各組織に総務部長（総務部長が置かれていない組織にあっては総務担当課長。）を長とする外局情報セキュリティ対策委員会を設置し、情報セキュリティポリシーの推進を図っています。

○　最高情報セキュリティ責任者

国土交通省における情報セキュリティ対策に関する事務を統括する責任を負っています。国土交通省では総合政策局長が務めています。

○　統括情報セキュリティ責任者

情報セキュリティ対策に係る連絡体制・関係規程の整備、行政事務従事者に対する情報セキュリティ教育の実施等、情報セキュリティ責任者を統括する責任を負っています。国土交通省では情報政策本部長が務めています。

○　情報セキュリティ責任者、情報セキュリティ担当官

情報セキュリティ対策に係る体制整備、自己点検票・実施手順の整備、自己点検指示等、所管する単位における情報セキュリティ対策に関する事務を統括する責任を負っています。国土交通省本省では情報セキュリティ責任者のみを設置し、大臣官房各課長・各局等総括課長が務めています。

また、特別の機関及び施設等機関では特別の機関及び施設等機関情報セキュリティ対策委員会の長である各機関の長が、地方支分部局においては各地方支分部局情報セキュリティ対策委員会の長である各地方整備局長、北海道開発局長、各地方運輸局長、各地方航空局長及び各航空交通管制部長が、外局においては各組織内に置いた情報セキュリティ対策委員会の長である総務部長が情報セキュリティ責任者を務め、情報セキュリティ担当官については各々の情報セキュリティ対策委員会の構成員（委員長を除く）及び支部を設置する場合は支部の長が務めています。

○　情報セキュリティ担当者

所管する事務や職員における情報の取扱いに関して判断する等、課室における情報セキュリティ対策に関する事務を統括する責任を負っています。国土交通省では各課室長が務めています。

○　システム管理者

セキュリティ機能の設計、利用手順書等の整備、安全区域の管理、所管する単位における情報システムごとの情報セキュリティ対策の管理等に関する事務を統括する責任を負っています。国土交通省では各課室長が務めています。

○　システム管理要員

定められた手順や規程に従い、所管する単位における情報システムごとの情報セキュリティ対策の実施について責任を負っています。

○　情報セキュリティ監査責任者

年度情報セキュリティ監査計画の策定、監査を実施する者に対する指示等、国土交通省における情報セキュリティ監査に関する事務を統

括する責任を負っています。国土交通省では情報政策本部長が務めています。

○　最高情報セキュリティアドバイザー
　情報セキュリティに関する専門的知識及び経験を有した専門家を置き、情報セキュリティ対策に関する様々な事務への助言等を行っています。

（２）情報セキュリティ対策に係る推進部署の体制

国土交通省では、総合政策局情報政策本部において、省内ＩＴ基盤整備・管理及び情報セキュリティ対策に係る事務を統括し、情報セキュリティ関連規程の整備や監査等を行っています。

３．３．監査等

省内における情報セキュリティ対策の実施状況を把握した上で必要な是正措置がとられていることを確認することを目的に、毎年度、情報セキュリティ対策に係る監査を実施しており、今年度は、下記の（１）から（３）に示す監査を実施しました。

(1) 情報セキュリティ対策実施状況の自己点検結果を踏まえた部局内監査

国土交通省は、地方支分部局や外局等を含め非常に大きな組織を有することから、各部局内で継続的、自律的に監査を行う部局内監査の仕組みを構築しています。部局内監査では、各部局において情報セキュリティ責任者が情報セキュリティ監査実施者を指名し、当該部局内における自己点検の結果を踏まえて必要な監査を実施することにより、情報セキュリティポリシー及び関係規程に準拠していることを確認します。

部局内監査を実施した結果、一部の部局において、情報の格付けと明示、格付けに基づいた取扱い、外部記録媒体使用時におけるウィルスチェックの徹底等といった分野について、一部取組が不十分な例があることが見受けられましたが、それ以外では特に大きな問題点はなく、概ね情報セキュリティポリシー及びその関連規程に則った運用が実施されていることが確認できました。なお、発見された問題点や課題については、当事者に対して速やかに対策を講ずるよう、指示が行われています。

(2)　今年度発生した障害・事故等事案への対応状況の確認

今年度発生した個人情報を含んだパソコンの盗難事案、メールアドレス漏えい事案、行政事務情報流出事案、インターネットへの不適切な画像掲載事案、サーバへの不正アクセス事案、Ｗｅｂページの不正改ざん事案について、本省の監査実施者が事後対策等の実施状況を書面またはヒアリングにより確認した結果、事後対策が適切に実施されていることが判明しました。

（3）行政情報ネットワークシステムのサーバにおける情報セキュリティ対策に関する監査

国土交通省が保有する情報システムについて、外部監査機関によるセキュリティ診断を計画的に実施しています。

具体的には、情報システムを構成するサーバやネットワーク機器に対して、ネットワークを通じての不正アクセスに関する脆弱性の検査、サーバの設定に関する検査を実施しました。その結果、いくつかの脆弱性が発見されましたが、速やかに対策を講じました。

４．情報セキュリティ対策の実施状況

４．１．省庁対策基準に関する自己点検結果

（１）自己点検についての課題と対策

（ア）自己点検について

情報セキュリティ対策は、国土交通省の情報セキュリティポリシー及びその関連規程等に基づいて、すべての職員が各自の役割を確実に実施することで実効性が担保されるものです。よって、情報セキュリティ対策の実施状況について、役割に応じた点検項目に基づき自らが実施状況を確認し、自己評価を行う自己点検を毎年度実施しています。自己点検を実施することにより、職員一人一人に自身の役割を再認識してもらうとともに、情報セキュリティに対する知識や意識の向上につながるものと考えます。

（イ）昨年度の課題と対策

昨年度の自己点検の結果から、情報の機密性に応じた格付けと取扱制限の明示が一部徹底されていない点が散見されたため、内部監査での指導及び今年度の自己点検実施時に情報の取扱制限について分かりやすくまとめた資料を、参照してもらうことで改めて情報の取扱制限を認識できるようにしました。

（ウ）対象者について

上記に示した目的等より、国土交通省においては、多様な職種で構成される職員全員（非常勤職員を含む）を対象として自己点検を実施しました。ただし、出張、休職等による長期不在の職員は非対象者としています。

（エ）回答方法について

自己点検は、役割ごとに作成された自己点検票に基づいて、各々が回答します。

回答者は、自己点検票の項目ごとに示されたセキュリティ対策事項の実施状況について、「実施している（実施）」、「概ね実施している（一部未実施）」、「実施していない（実施不足）」等の中から適切なものを選択して回答します。

（２）自己点検結果の状況

（ア）国土交通省全体の把握率

今年度の国土交通省全体における自己点検対象者のうち、対策実施状況が把握できた者の割合である把握率※1は、１００％となりました。

※1：「情報セキュリティ報告書専門委員会 報告書（２００９年９月１１日）」においては、把握率は「報告対象とした者のうち、対策実施状況が把握できた者の割合」と定義されています。

（イ）国土交通省全体の実施率

今年度の国土交通省全体における自己点検の実施率は、下記の図２のとおりとなりました。なお実施率※2 とは、対策実施状況が把握できた者のうち、点検項目ごとに「実施」と回答した者の割合を、全点検項目に対して平均したものです。

※2：「情報セキュリティ報告書専門委員会 報告書（２００９年９月１１日）」においては、実施率は「把握した者のうち、責務が生じた者に占める対策を実施した者の割合」と定義されています。

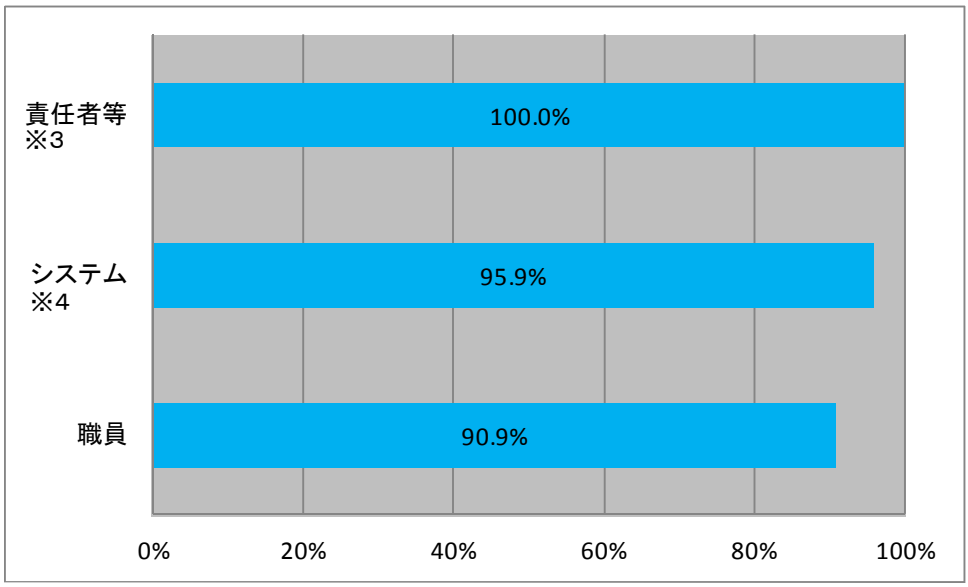

図２　役割別の実施率

※3：最高情報セキュリティ責任者、情報セキュリティ監査責任者、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ担当者等

※4：システム管理者、システム管理要員等

実施率に関しては、全体的に９０％を超える高い結果となっており、組織としての情報セキュリティ管理の運営、並びに情報システムの構築や運用等、ライフサイクル全体に渡る情報セキュリティについて、対策が進んでいることが分かりました。一方、「職員」については、情報の格付けの決定と格付けに従った取扱いに関して比較的低い水準となっていることが分かりました。

（ウ）国土交通省全体の到達率

今年度の国土交通省全体における自己点検の到達率※5 は、下記の図３のとおりとなりました。

なお到達率とは、点検項目ごとの「実施」の割合が一定の値以上に達し

ている点検項目の数が、全体の点検項目数に対してどの程度の割合を占めているかを示したものです。例えば「到達率１００」とは、点検項目ごとの「実施」の割合が１００％であるもの、すなわち、すべての回答者が「実施」と回答した点検項目が、全体の点検項目の中でどの程度を占めているかを示します。同様に、「到達率９５」及び「到達率９０」とは、点検項目ごとの「実施」の割合が、それぞれ９５％以上の点検項目及び９０％以上の点検項目の数が、全点検項目数の中でどの程度を占めているかを示します。

※5：「情報セキュリティ報告書専門委員会 報告書（２００９年９月１１日）」においては、到達率は「把握した者のうち、責務が生じた一定の割合（１００％、９５％、９０％）以上の者が対策を実施した遵守事項の割合」と定義されています。

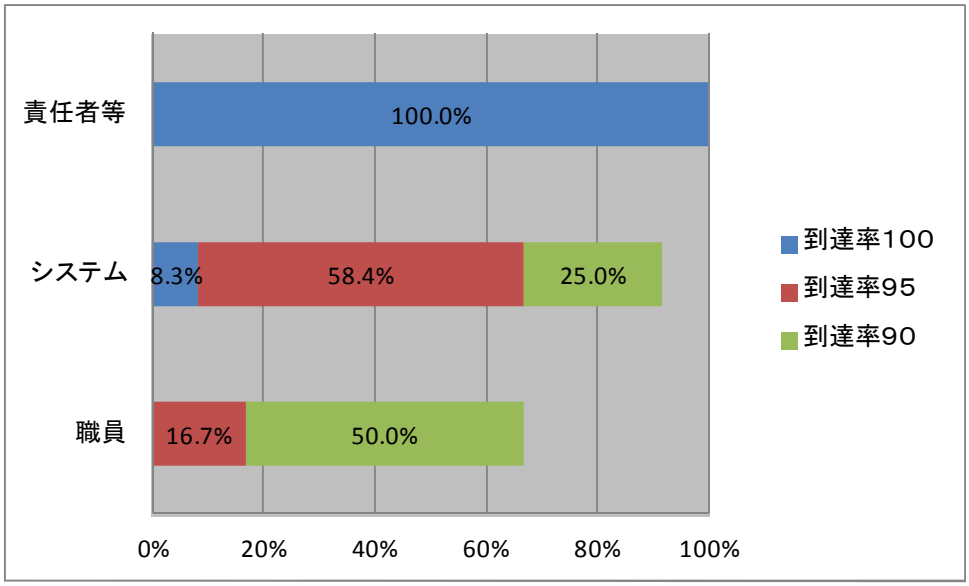

図３　役割別の到達率

到達率に関しては、「９０％の実施率に到達した点検項目の割合（到達率９０）」については、「職員」を除いて、高い水準を確保している一方で、「１００％の実施率に到達した点検項目の割合（到達率１００）」については、「責任者等」を除いて全体的に比較的低い水準に留まっています。「職員」の到達率が低い水準となったのは、（イ）で記載したとおり、格付けの決定や格付けに従った取扱い等において全般的に低い水準となっていたことが原因と考えられます。

（３）総評

今年度の情報セキュリティ対策の自己点検結果は、各役割別の把握率が１００％に達し、これまで行ってきた情報セキュリティに関する周知徹底により意識が向上した成果と考えています。また実施率についても各役割別でそれぞれ９０％を越えており高い水準を維持できていました。しかしながら行政事務従

事者を対象とした自己点検では情報の格付けの決定と格付けに従った取扱いに関して比較的低い水準となっており、適切な運用に関する分かりやすい周知に重点を置いた更なる周知徹底を行う必要性があると考えています。

４．２．情報システムごとの状況

（１）課題と対策

情報システムの情報セキュリティ対策が不十分な場合、重要な情報の漏えい、改ざん、破壊等が発生する要因となる可能性があります。よって、内閣官房情報セキュリティセンター（以下、「ＮＩＳＣ」という。）では、全府省庁における情報システムの対策実施状況を明らかにするために、重点検査を実施しています。具体的には、各府省庁が運用する情報システムについて、それらが政府統一基準で定められている遵守事項に則った対策を実施しているかを、ＮＩＳＣが配布した調査様式に基づいて内部調査を実施します。

今年度は、情報システムを構成する公開Ｗｅｂサーバ、電子メールサーバについて、重点検査を実施しました。

（２）情報システムの対策状況

（ア）公開Ｗｅｂサーバ

公開Ｗｅｂサーバの OS 及びサーバアプリケーションのセキュリティアップデート対応についての実施状況は、すべて１００％でした。

（イ）電子メールサーバ

電子メールサーバの OS 及びサーバアプリケーションのセキュリティアップデート対応についての実施状況は、すべて１００％でした。

（３）総評

今年度の情報システムにおける重点検査の実施結果は、公開用Ｗｅｂサーバ、電子メールサーバのすべてについて１００％となりました。今後についてもこの状態を維持できるように、引き続き政府統一基準群及び情報セキュリティポリシーに基づく情報セキュリティ対策を実施します。

４．３．教育・啓発

情報セキュリティの向上は、組織の社会的信頼を守り、職員一人一人が安心して業務に従事することにもつながります。情報セキュリティ対策に取組むためには、各職員が情報セキュリティ対策を理解し、適切に実践していく必要があります。

国土交通省では、下記の取組を通じて職員に対する教育・情報提供等を実施しています。

（１）職員への情報提供

国土交通省では、職員が守るべきルールを情報セキュリティポリシーや「国土交通省行政情報システム管理運営規則」として定め、情報セキュリティに関する情報をいつでも全職員が確認することができるようにイントラネット経由で省内職員に配信しています。また、情報セキュリティポリシーの中から特に重要なポイントについて「情報セキュリティ確保のためのお役立ち５つのポイント」として整理し、職員に対して適宜、ＰＣにポップアップメッセージを表示すること等により周知徹底しています。さらに、職員向けの分かりやすいＰＣ利用に関する情報であるヒント集（パスワード設定方法、暗号化の方法、データのバックアップ方法、ＣＤへのデータ書込み方法、ウィルスチェック方法）についてもイントラネットに掲載しています。

また、不審メール対策として省庁職員になりすまして送信される不審メールを開封するとウィルスに感染するおそれがある旨を示したポップアップメッセージを表示し、職員に対して注意喚起を行うとともに、外部から受信する全メールに対し、一定の基準によりシステムで自動破棄やメッセージ本文に注意喚起文を挿入し、セキュリティの確保に努めました。併せて、標的型メール攻撃に関する教育・意識啓発のため、同攻撃に対し適切な対処が出来ることを目的とした擬似メールを用いた訓練を実施しました。

さらに、随時発生したセキュリティ事案を引用し、全職員に対し事例解説を含めた情報提供による注意喚起を行いました。

（２）教育・研修

職員に対する研修としては、今年度は５月及び１１月に情報ネットワーク・セキュリティ基礎研修を実施し、「行政情報システムの運用・管理の知識を必要とする職員」を対象に、「国土交通省情報セキュリティポリシーの概要」について講義を実施しました。また、地方支分部局の職員向けの研修の中にも、一部、国土交通省における情報セキュリティの概要等について講義する内容を取り入れています。

同様に、部局毎の独自の取組として、例えば、気象庁では階層別研修や専門分野ごとの研修カリキュラムの中に情報セキュリティに係る講義を組み込んで実施し、情報セキュリティの部内監査の際に、併せて情報セキュリティの講演会を実施しています。国土地理院においては、毎年度３回程度情報セキュリティ講習会を実施し、全職員が受講するように努めています。

また、情報システム調達時に情報セキュリティを企画・設計段階から確保するための方策である Security by Design について、省内関係者に対しＮＩＳＣによる研修会を開催しました。

４．４．調達・外部委託

情報処理業務を外部委託により行う場合には、委託先における業務の遂行を委託元が直接に指揮命令することがなく、また当該業務に必要な情報を委託元から提供して委託先に取扱わせるため、情報セキュリティを確保する観点から、委託元としての業務を行う者が委託先による業務の遂行を契約等により適切に管理する必要があります。

そのため国土交通省では、情報処理業務を外部委託により行う場合に、委託元としての業務を行うシステム管理者が遵守すべき事項を定め、外部委託により行う情報処理業務の遂行において必要な情報セキュリティ水準を確保することを目的として、「外部委託における情報セキュリティ対策実施規程」を定めています。なお、当該規程については、イントラネットに掲載すること等により、各職員へ周知しています。

４．５．その他取組んだ事項

政府機関の情報システムの効率的・継続的な情報セキュリティ対策の向上を図り、「事故前提社会」への対応力を強化する観点から策定された、第２次情報セキュリティ基本計画(平成２１年２月３日情報セキュリティ政策会議決定)に基づき、災害・障害時対応の必要性・優先度を勘案し必要なものについて、業務継続計画の策定を進めています。

５．情報セキュリティに関する障害・事故等報告

５．１．情報セキュリティに関する障害・事故等の把握

国土交通省においては、万一情報セキュリティに関する障害・事故等が発生した場合、「障害・事故等報告及び対処手順』及び緊急連絡網に基づき対処することと定めています。具体的には、行政事務従事者が情報セキュリティに関する障害・事故等を発見した場合、障害・事故等の内容に応じてシステム管理者または情報セキュリティ担当者に報告を行います。報告を受けたシステム管理者または情報セキュリティ担当者は、情報セキュリティ責任者の承認の下、対処の指示及び関係者への連絡を行います。さらに、対処完了後に再発防止策を策定した上で、統括情報セキュリティ責任者に報告することとなっています。

５．２．情報セキュリティに関する障害・事故等の把握

平成２３年度における情報セキュリティに関する障害・事故等の概要については、以下のとおりです。

（１）事案Ⅰ

平成２３年６月１０日にモバイルパソコンを入れたバックの盗難が発生した。個人情報が含まれたファイルを保存していたために、個人情報が流出したおそれがあり盗難の届出と当該端末からのネットワークへのアクセスを無効化した。再発防止策として、個人情報の厳重な管理（パスワード設定・暗号化）を周知徹底した。

（２）事案Ⅱ

平成２３年６月２７日に送信先である多数のメールアドレスが表示されたままの状態で誤ってメールを送信した。当該メールの受信者に他の受信者のメールアドレスが通知される事態となった。送信先には直ちに報告とお詫びを行い、当該電子メールの削除を依頼した。再発防止策として、不特定多数の者に電子メールを送信する際には複数の者による確認を実施することとした。

（３）事案Ⅲ

平成２３年７月２０日にプログラムの脆弱性を利用するコンピュータウィルスにパソコンが感染した。感染したパソコンを経由し、サーバからユーザ情報を抜き取られた可能性があるためサーバを切り離し、運用を停止するとともに直ちにウィルスの駆除をおこなった。また、個人情報が含まれたファイルを保存していたため個人情報が流出したおそれがあり、サーバのネットワークからの切り離しと関係者への報告とお詫びを行った。再発防止策として、サーバ上の対策状況とパソコンにおけるセキュリティ対策状況の再確認を行った。

（４）事案Ⅳ

平成２３年９月５日に非公開の扱いとされている情報等を撮影した写真が、個人のホームページにおいて公開されていたことが判明した。掲載者の特定とともに、掲載者による写真の削除及びホームページの閉鎖を実施した。再発防止策として格付けの見直しや情報管理体制等の情報セキュリティ対策を強化した。

（５）事案Ⅴ

平成２３年１０月２７日にサーバが不正に侵入され、他機関のサーバに対し当該サーバを踏み台とした攻撃が行われたことが判明した。このため、侵入されたサーバを切り離し、運用を停止するとともにＩＤ及びパスワードの変更やアクセス回数の制限といった設定の変更を行った。再発防止策として、管理している各サーバ等の設定状況の確認をおこなった。また、ファイヤウォールの設定状況を再確認した。

（６）事案Ⅵ

平成２３年１２月２０日に一部のＷｅｂページが不正に改ざんされていたことが判明した。当該サーバを含め類似サーバをネットワークから切り離し、運用を停止した。再発防止策として、当該機関における外部公開サーバ類の総点検と脆弱性検査を実施した。

６．情報セキュリティ対策に関する次年度の計画

平成２４年度に予定している情報セキュリティ対策については、今年度に引き続き自己点検や監査等を着実に実施するとともに、一層の充実を図るために特に以下の事項について重点的に取組んで参ります。

（１）情報の格付けに応じた適切な取扱い

情報の不適切な利用や持ち出し等による情報漏えいを防止するため、ライフサイクルごとに情報の格付けに応じた適切な取扱いの徹底を行います。

（２）自己点検・監査実施方法の改善

情報セキュリティを取り巻く環境の変化に応じた点検項目の設定や点検内容を正確に理解してもらうために更なる見直しを行います。また、外局や地方支分部局を含め省内全ての部局において実施している部局内監査について、より効率的・効果的なものとなるよう見直しを行います。

（３）情報セキュリティ教育

情報セキュリティ対策の実施効果を一層高めるためには、全職員に対して対策や措置内容を分かりやすい形で周知・徹底することが重要です。職員に対し従前より実施している「情報セキュリティ確保のためのお役立ち５つのポイント」や不審メール対策に関する周知等について、内容の改善も図りながら今後も継続的に実施します。

７．おわりに ～最高情報セキュリティアドバイザーからのメッセージ～

国土交通省では、情報セキュリティポリシーの制定及びその運用を中核とする情報セキュリティ対策を実施しています。国土交通省は、多くの外局や地方支分部局を有する巨大な組織であり、業務内容や取扱う情報も部局によって多様であります。昨今の情報セキュリティへのリスクの高まりをうけて、この６万人の職員全員において情報セキュリティ対策をいかに適切に実施していくかが重要な課題です。

これまでにも、国土交通省では、職員が順守すべき５点のポイントを繰り返し周知、効率的に自己点検を実施、点検結果を把握するための工夫、各部局における自律的な監査の取組など、成果を上げてきました。この大きな組織でより効率的、効果的に情報セキュリティ対策の徹底を図るための取組を行うとともに、ＣＩＳＯ配下に約７０名の情報セキュリティ責任者及び約４，５００名の情報セキュリティ担当者等による情報セキュリティ対策に係る体制を構築して参りました。

今年度の自己点検においては、把握率１００％を達成できたことは、上記で述べた巨大な組織における情報セキュリティ対策の推進体制が構築されていること、効果的な教育・啓発により醸成された多くの職員の高いセキュリティモラルが背景となっています。情報セキュリティ対策を推進するには、職場における良好な人間関係、信頼関係を基礎としつつ、形式的な処理によることなく、各部局において取扱う情報の内容や業務の実態を踏まえ、柔軟かつ適切な対策・措置の運用を図ることが重要です。

今後も、職員に対する効果的な教育・啓発、新たな脅威への速やかな対策の実施等、情報セキュリティ対策を継続的に実施して参ります。

国土交通省最高情報セキュリティアドバイザー
日野　弘